RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: SVB-T10

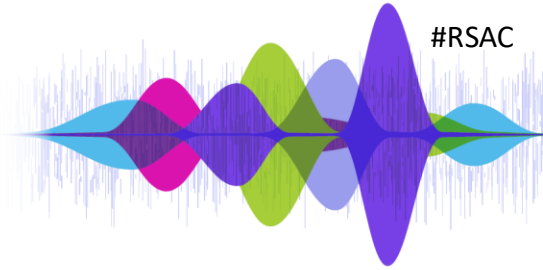
What's in the Box? Hardware Bill of Material and what it means.

Cassie Crossley

Vice President, Supply Chain Security
Schneider Electric
linkedin.com/in/cassiecrossley

Allan Friedman, PhD

Adjunct Professor
Luddy School of Informatics, Computing, & Engineering
Indiana University
linkedin.com/in/allanafriedman



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

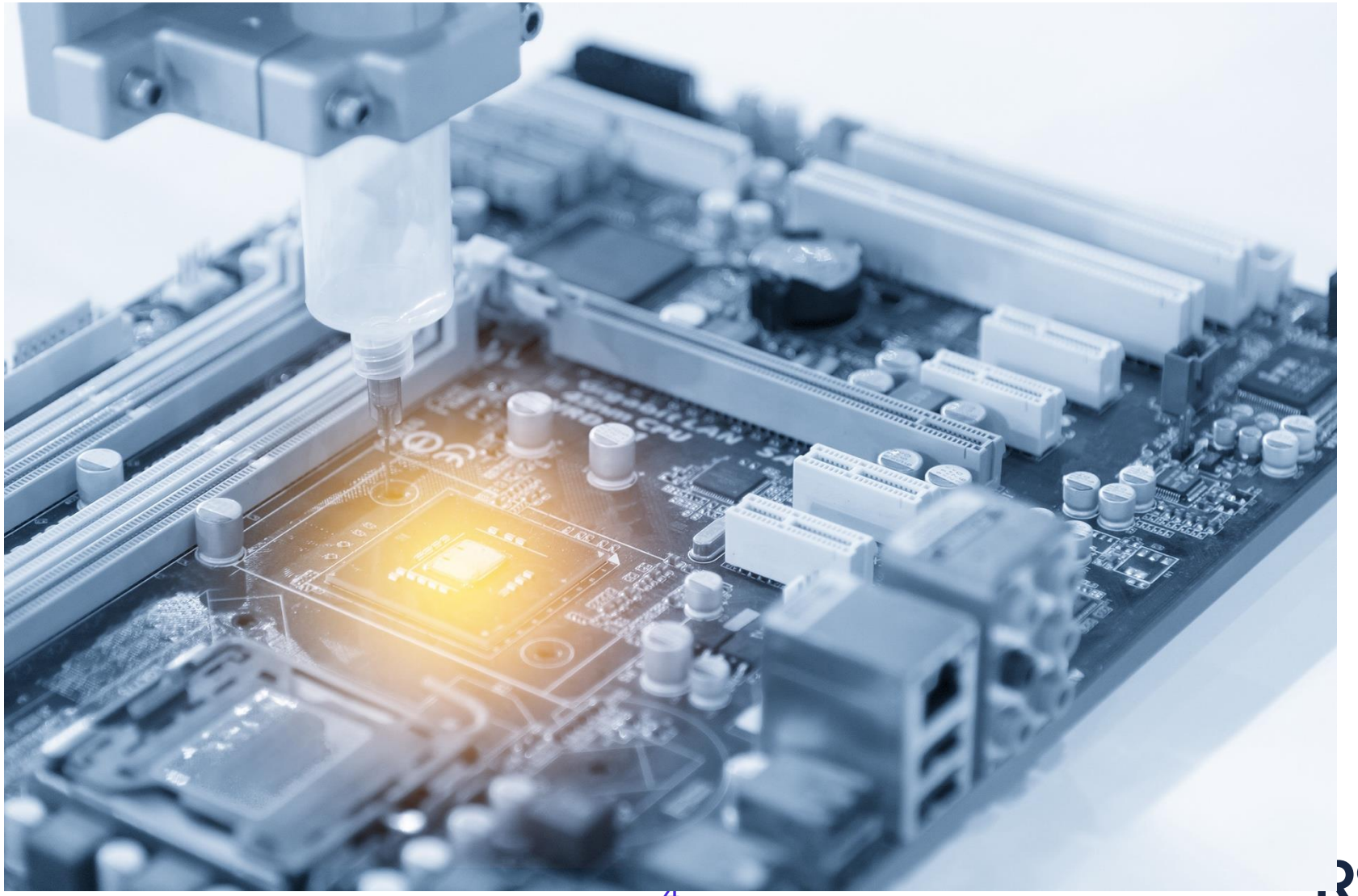
© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Allan Friedman is speaking in his capacity as a Research Scientist with Indiana University. He is in no way representing the Cybersecurity and Infrastructure Security Agency or the US Government.

Cassie Crossley is speaking in her capacity as an industry champion in product security and supply chain security. Any statements are her own and may not represent Schneider Electric.

Today, we'll be talking about THINGS

And what's in them

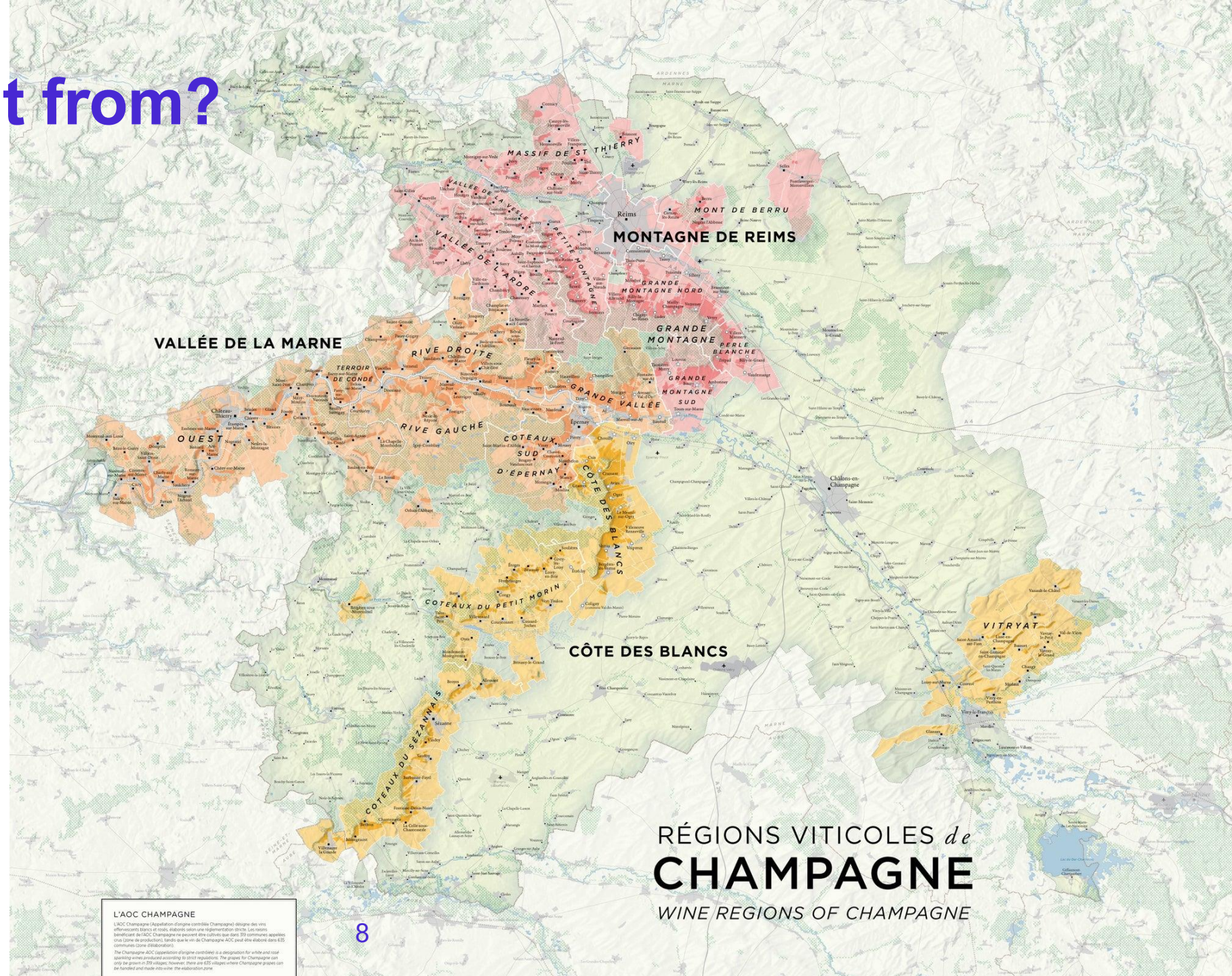


But sometimes we like to talk about wine

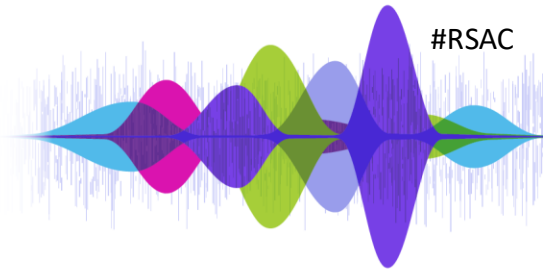
Yeah, but what is it?

No, like what *is* it?

But where is it from?



Paying attention
vs
Getting hands on in a Sandbox?



- Building things
- Risks in things
- What might it look like?
- HBOMs in practice

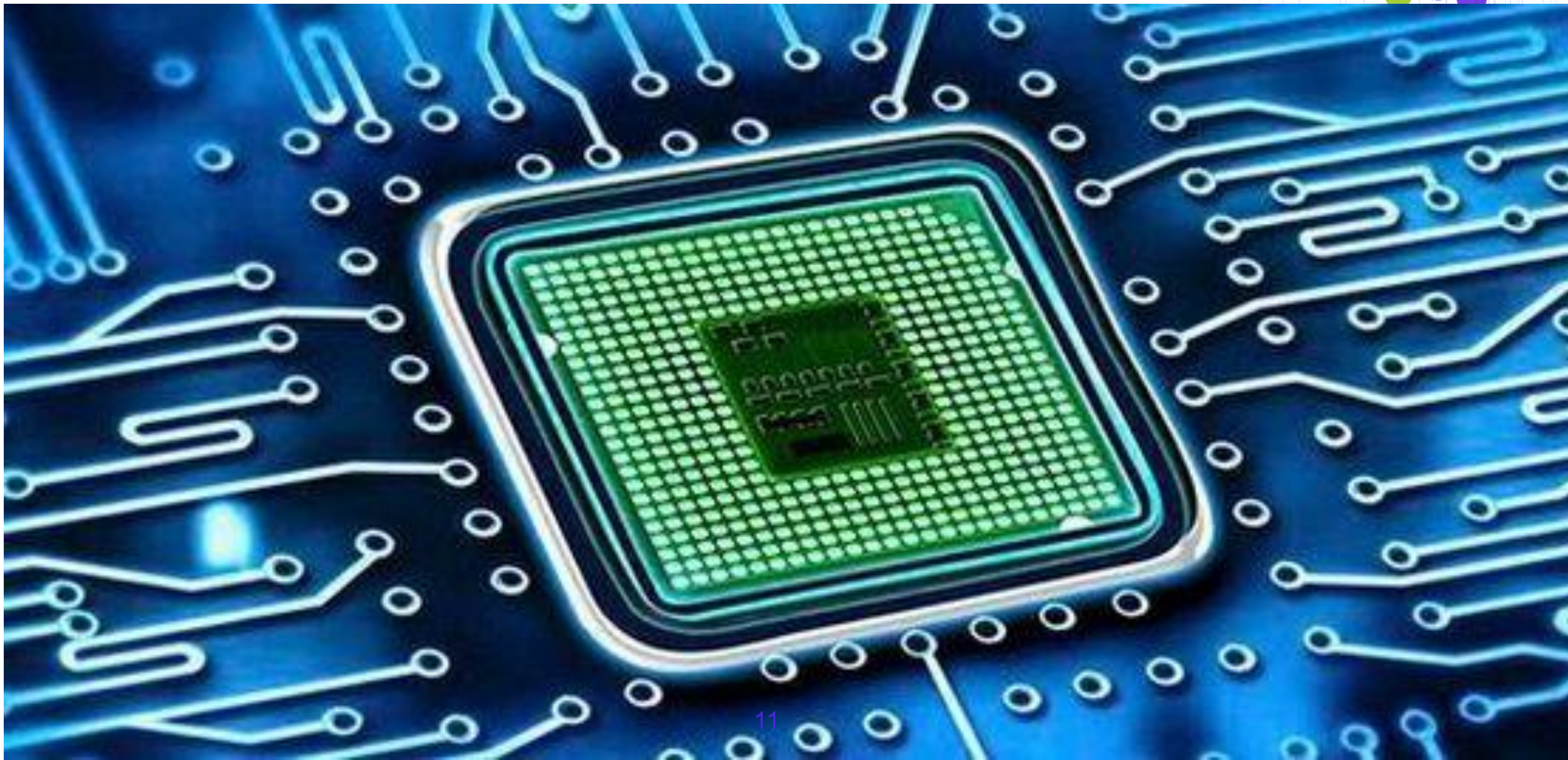
RSAC 2025 Conference

We all know about SBOM

But did you know that THINGS are built from STUFF?

Many Voices.
One Community.

Software runs on Semiconductors



Good News – Can’t build a THING without a BOM

- Logistics chains have always been a part of manufacturing
- Modernization has pushed for greater efficiency
- Quality requires data and effective management

BOMs in Practice

RSAC 2025 Conference

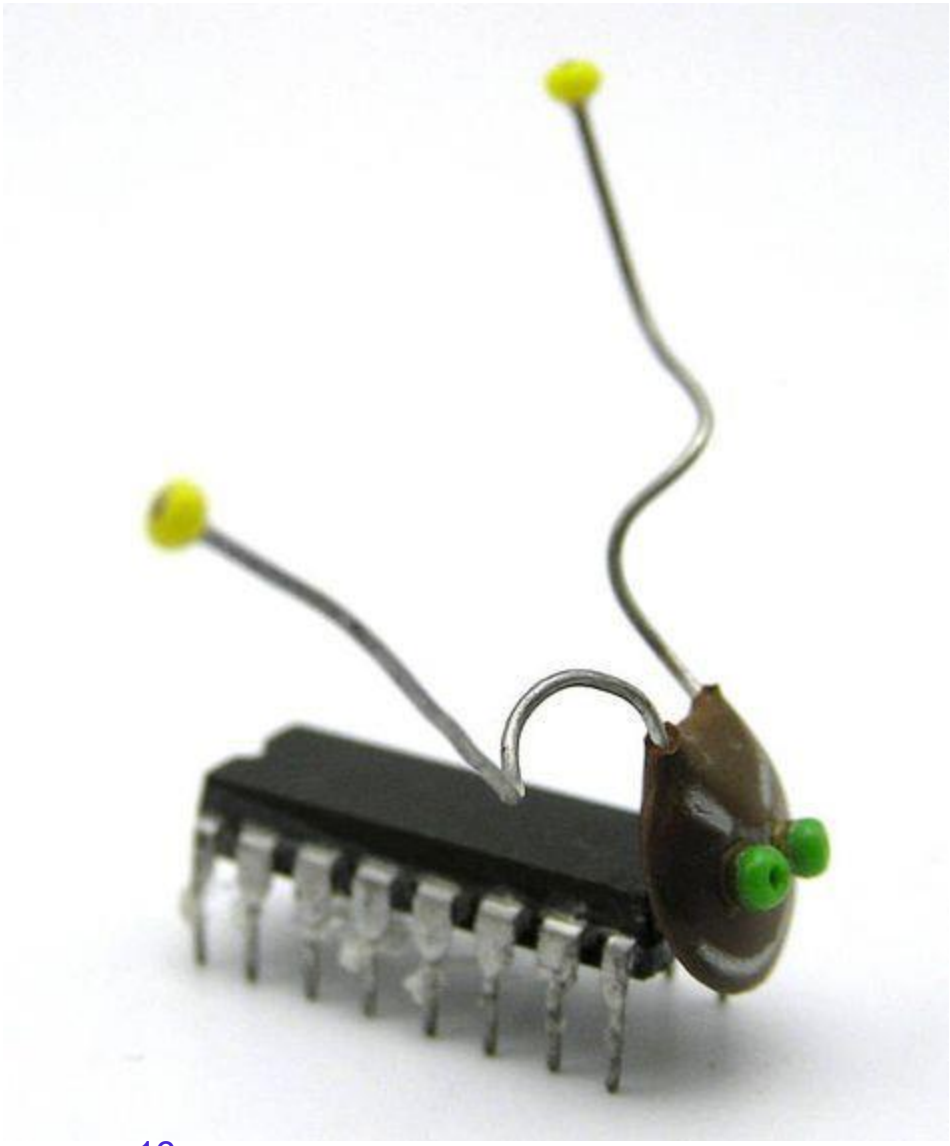
Bad News

A traditional BOM may not be enough

Many Voices.
One Community.

Vulnerabilities

- Downfall
- Augury
- LeftoverLocals



Counterfeits

Active Tampering

Pagers attack brings to life long-feared supply chain threat

Eva Dou and Gerrit De Vynck Washington Post

Published 11:02 a.m. ET Sept. 19, 2024

Forbes

DAILY COVER

Silicon Valley's Military Drone Companies Have A Serious 'Made In China' Problem

By David Jeans, Forbes Staff. Senior writer covering tech, defense

Apr 16, 2025, 06:30am EDT, Updated Apr 17, 2025, 01:31am EDT

Goals of an BOM – “Known Badness”

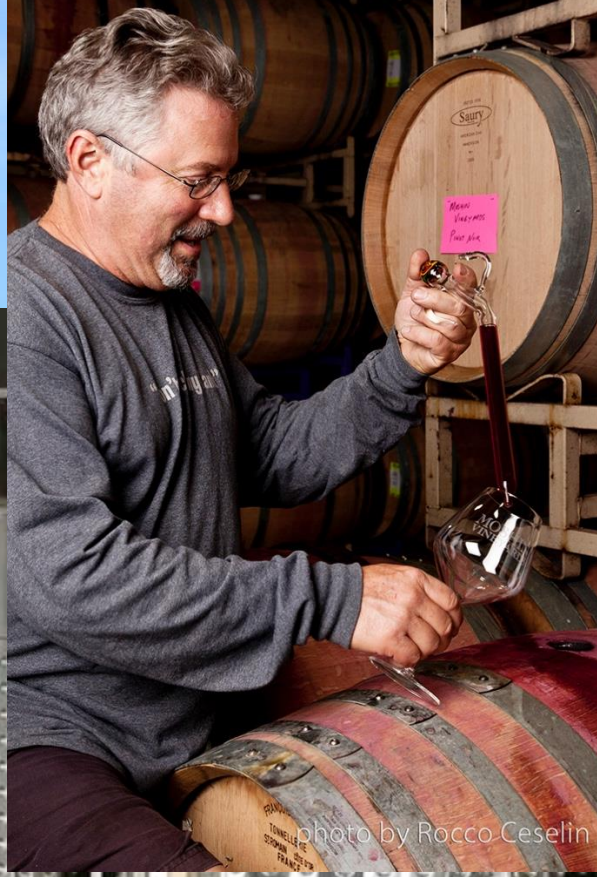
Countries matter

FOCI

Compliance

- Sanctions
- Regulations
- Tariffs
- Import/Export controls

Provenance



Goals of HBOM – Supply Chain Visibility

- Tracking across the supply chain down to customers or pre-sale regulatory compliance
- Consistent and repeatable
- Reliable and predictable
- Portable
- Automatable
- Auditable

Scope

Security domain

Provide metadata to make decisions about the origins and security risks of a given product

Semiconductors

Digital components

“store, process, transmit”

Not focusing on other supply chain topics

But need to be able to integrate with those efforts

Cross sector

- Defense
- Energy
- Telecommunications
- Automotive
- Medical Devices
- Manufacturing

Who – More than nerds

- Business
- Procurement
- Supply Chain
- Logistics
- Legal
- Compliance
- Suppliers

What would this mean in Practice

Date specific

Location specific

Services

Chain of custody

Subcomponents and assemblies

Gubmints gonna Gubmint

- Regulations are coming

Gubmints gonna Gubmint

- Regulations are here

RSAC 2025 Conference

Good news
Not starting from scratch

Starting Point: An HBOM Framework

Published by CISA's National Risk Management Center & Communications and IT Sector Coordinating Councils in 2023

- Describes manufactured goods made up of assemblies comprising components
- Offers a set of basic roles for actors in the supply chain
- Presents a simple taxonomy of field names and basic details

Explicitly Documented Use Cases

Compliance

- Government
- Customer requirements
- Internal quality controls

Security

- Risks from entities and jurisdictions
- Component risks

Availability

- World events
- Clustering and concentration

Gaps

- Linking HW and SW
- Provenance
- Trust
- Measurement and auditing
- Specific implementations

Integrating into existing efforts and standards

- CycloneDX BOM specifications
- SPDX Hardware-specific HBOM model
- Trusted Computing Group’s Platform Certificates
- Proprietary standards from enterprises and supply chain experts
- Coming soon from a major manufacturing association

Identifiers

- Global identifiers are a hard problem.
  - SKU / lots / relabeling
  - We don’t even have them for software
- Numerous existing naming schema are used widely
- AI might be able to help

Should this data be secret?

Who gets to see all my data?

- Very good reasons to not have public supply chain data on everything
- Access control
- Third party verification
- Auditability
- Goal: attestations around what is NOT in my supply chain

Attestations (noun?)

Legal

Technical

“On behalf of the above-specified company, I attest that, to the best of my knowledge, [software producer] presently makes consistent use of the following practices…”

An attestation is a cryptographically signed collection of machine-generated claims related to one or more software artifacts or events

Auditability and conformity

Legal

Technical

Learning from the software bill of materials work

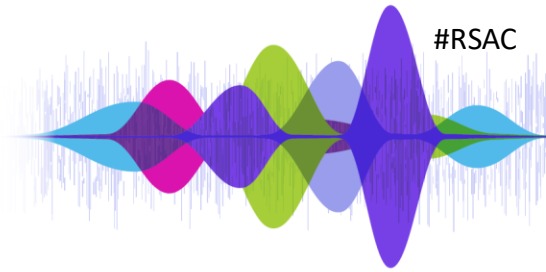
- Versioning matters
- Data matters – buildable today, but aim for high quality input
- Challenge – hard to patch, even longer tail
- Mitigations are possible, but may require firmware shims
- Mapping from asset management to contents

- You have to build a community of practice

Importance of a transparency layer

- Common approach to tracking data
- Plan for interoperability of standards
- Build in business processes
- Separate data from policy
- **Transparency is the first step - and often the most valuable**

“Apply” Slide



- Today – consider the risks across your organization from hardware
  - Intentional attacks
  - Vulnerabilities or
  - REGULATION
- By the time Black Hat rolls around…
  - Explore existing tools and frameworks for tracking hardware
  - Ask at least one core supplier of hardware about their HBOM capabilities
  - Stay tuned for an effort to build something coordinated across sectors

RSAC™ | 2025 Conference

Many Voices.
One Community.